(pset3) Part 2: Function Proofs

👈 Back to problem set index.

Problem Three: Strictly Increasing Functions

A function $f : \mathbb{Z} \to \mathbb{Z}$ is called ***strictly increasing*** if the following statement is true about f:

$$\forall x \in \mathbb{Z}. \forall y \in \mathbb{Z}. (x < y \to f(x) < f(y)).$$

Strictly increasing functions have a bunch of nice properties.

i. Is the function $f : \mathbb{Z} \to \mathbb{Z}$ defined as $f(x) = x^2$ strictly increasing? How about if we defined it as $f(x) = x^3$? No justification is necessary.

ii. Let $f : \mathbb{Z} \to \mathbb{Z}$ and $g : \mathbb{Z} \to \mathbb{Z}$ be arbitrary strictly increasing functions. Prove that $g \circ f$ is strictly increasing.

This is a proof of the form "any object with property X also has property Y." Look back at the lecture examples involving involutions for some guidance about how to proceed here.

Make sure to distinguish what you're assuming from what you're proving. Introduce variables when you're asked to prove a universally-quantified statement, and don't introduce them when you're assuming a universally-quantified statement.

iii. Let $f : \mathbb{Z} \to \mathbb{Z}$ be an arbitrary strictly increasing function. Prove that f is injective.

If you have two integers x and y where $x \neq y$, then you know either that $x < y$ or that $y < x$. If x and y are otherwise arbitrarily chosen, you can avoid doing a proof by cases by using this magic phrase:

"Assume, without loss of generality, that $x < y$."

*This phrase tells the reader "dear reader, who I am sure is well-dressed, very refined, and very classy, there really isn't a difference in the logic between the cases where $x < y$ and $y < x$. Therefore, to avoid boring you, I'm going to just prove one of those two cases. And since you are so Smart and Wise and Funny, you **surely** are smart enough to see what the other case would be, because it's literally the same except that we swap the roles of x and y." It's a great way to cut down on the amount you have to write without losing anything.*

You can use this phrase in other contexts where there are two symmetric choices. Just make sure that those cases really truly are identical except for which variable plays which part!

Problem Four: Eventual Bijections

Suppose you have a function $f : A \to A$ from some set back to itself. This allows us to compose f with itself multiple times. To make things a bit easier to talk about, let's introduce some notation. For any natural number n, we'll define $f^n : A \to A$ to be the function $f \circ f \circ \cdots \circ f$, with f appearing n times in the expression. So, for example, f^1 is just the function f itself, while f^2 is the function $f \circ f$ and f^3 is the function $f \circ f \circ f$. As a special case, we'll say that f^0 is the function $f^0(x) = x$; this is chosen to make things behave more consistently.

i. Let $f : \mathbb{Z} \to \mathbb{Z}$ be the function $f(n) = 2n - 1$. Fill in the blanks below. No justification is required.

1. $f^3(2) =$ _____
2. $f^{137}(1) =$ _____
3. $f^0(137) =$ _____

In many cases, if you know something about how a power of a function works, you can learn something about the function itself.

ii. Let $f : A \to A$ be a function. Prove that if f^3 is surjective, then f is surjective.

Make sure you're proving the right thing. Here, you know something about f^3, and your goal is to infer something about f itself. Make sure not to instead assume f is surjective and prove f^3 is surjective; that follows from what we proved in lecture and is a different argument.

This is a great place to write out what it is that you're assuming and what it is you're proving. Much of the complexity of this problem stems from differentiating between the two.

iii. Let $f : A \to A$ be a function. Prove that if f^3 is injective, then f is injective.